Política de Detecção de Vulnerabilidades para o Setor de Defesa e Aeroespacial

Baseado no Framework NIST 800-53 (RMF)

2. Propósito

Estabelecer um processo contínuo para identificar e avaliar vulnerabilidades em sistemas de informação e ativos de informação do setor de defesa e aeroespacial, a fim de proteger a confidencialidade, integridade e disponibilidade de dados críticos e sistemas de missão.

3. Escopo

Esta política se aplica a todos os sistemas de informação e ativos de informação do setor de defesa e aeroespacial, incluindo:

- **Redes:** Redes de computadores, incluindo redes classificadas e não classificadas.
- **Dispositivos:** Computadores, servidores, dispositivos móveis, dispositivos IoT e outros dispositivos conectados.
- **Aplicações:** Softwares e aplicações utilizados em sistemas de missão e sistemas de suporte.
- **Dados:** Informações confidenciais, dados de missão, dados de voo e outros dados críticos.

4. Política

O setor de defesa e aeroespacial se compromete a:

- **Realizar varreduras regulares de vulnerabilidades:** Identificar e avaliar periodicamente as vulnerabilidades existentes em seus sistemas de informação.
- **Priorizar e remediar vulnerabilidades:** Priorizar a correção das vulnerabilidades de acordo com o seu nível de risco e impacto potencial nos negócios.
- **Documentar e reportar:** Documentar os resultados das varreduras de vulnerabilidades e reportar à alta gerência os riscos e as medidas de remediação tomadas.

5. Procedimentos Relacionados

- **Planejamento:**
  - Definir a frequência das varreduras de vulnerabilidades.
  - Selecionar ferramentas e métodos adequados para a análise.
  - Identificar os sistemas de informação a serem analisados.
- **Execução:**
  - Realizar a varredura de vulnerabilidades de acordo com o plano.
  - Documentar os resultados da varredura, incluindo as vulnerabilidades identificadas, seu nível de risco e as medidas de remediação recomendadas.
- **Remediação:**
  - Priorizar a correção das vulnerabilidades de acordo com o seu nível de risco e impacto potencial nos negócios.
  - Implementar medidas de remediação adequadas para cada vulnerabilidade.
  - Monitorar a efetividade das medidas de remediação.
- **Relatório:**
  - Reportar à alta gerência os resultados das varreduras de vulnerabilidades e as medidas de remediação tomadas.

6. Não Conformidade

O não cumprimento desta política poderá resultar em medidas disciplinares, incluindo advertência verbal, advertência escrita, suspensão ou rescisão de contrato.

7. Compromisso/Autoridade da Gestão

A alta gerência do setor de defesa e aeroespacial se compromete a fornecer os recursos necessários para a implementação e o cumprimento desta política. A equipe de segurança da informação é responsável pela gestão e atualização da política.

8. Cronograma de Revisão

A política será revisada anualmente ou após um incidente de segurança cibernética significativo.

9. Definições

- **Vulnerabilidade:** Fraqueza em um sistema de informação que pode ser explorada por um invasor para obter acesso não autorizado, comprometer a integridade dos dados ou interromper o serviço.
- **Detecção de vulnerabilidades:** Processo de identificação de vulnerabilidades em um sistema de informação.
- **Plano de remediação:** Plano que define as medidas a serem tomadas para corrigir as vulnerabilidades identificadas.

Observações:

- Esta política é um exemplo e deve ser adaptada às necessidades específicas do setor de defesa e aeroespacial.
- É importante consultar especialistas em segurança cibernética para a implementação da política.